Mishap Investigation

Safety Directors Meeting
February 1, 2006

Faith Chandler
Office of Safety and Mission Assurance

Investigating Mishaps - Topics

1. NASA Procedural Requirements (NPR) 8621.1 Changes
2. Causes of Type A Mishaps
3. Open Investigations

NPR 8621.1: Mishap Reporting, Investigating and Recordkeeping - Overview

- **Describes how to respond to a mishap and close call from discovery through corrective action closure.**

- **Includes:**
  - **Descriptions of roles and responsibilities**
  - **How to classify mishaps (based on dollar loss, injury & visibility)**
  - **How to establish an investigating authority**
  - **How to perform an investigations & generate a report**
  - **How to endorse a report and authorize it for public release**
  - **How to complete corrective actions and generate lessons learned**
  - **How to retain records**

The purpose of NASA mishap investigation process is to determine cause and develop recommendations to prevent recurrence.

Overview: Changes to NPR 8621.1

NODIS review begins this week: January 31.

Updates:

- **Incorporated requirements from Administrator's policy letter:**
  - **Center Director (CD) personally reports Type A mishaps, Type B mishaps and Type C lost time cases to administrator in 24 hours.**
  - **CD personally reports serious injuries and fatalities (off site when it becomes known)**
- **Updated titles of personnel and organizations**

Overview: Changes to NPR 8621.1
Mishap Investigation Notional Timeline

Immediately – 24 hours
Safe Site, Initiate Pre-Mishap Plans, Make Notifications, Classify Mishap,

Two Changes

Within 48 Hours of Mishap
Appoint Investigating Authority

Within 75 Workdays of Mishap
Complete Investigation & Mishap Report

Within An Additional 30 Workdays
Review & Endorse Mishap Report

Within An Additional 5 Workdays
Approve or Reject Mishap Report

Within An Additional 10 Workdays
Authorize Report For Public Release

Within An Additional 10 Workdays
Distribute Mishap Report

Concurrent
Within 15 Workdays of Being Tasked
Develop Corrective Action Plan
Within 10 Workdays of Being Tasked
Develop Lessons Learned

Within 145 days of mishap

Overview: Changes to NPR 8621.1

Not a Mishap

- **If weather (e.g., hurricane) or natural phenomenon (e.g., earthquake) is the proximate cause - not classified as a mishap**

- **A failure resulting in damage to flight hardware during the ground Acceptance Test Procedure (ATP) is not a mishap when all of the following are true:**
  - **a. The failure is a predictable outcome.**
  - **b. Only the flight article is damaged or failed, and testing did not damage the test stand, or facility or cause personnel injury.**
  - **c. The test equipment functioned properly.**
  - **d. There were no anomalies in the facility or test procedures that could have contributed to the article failure.**
  - **e. The test team performs a test failure analysis that identifies the root cause(s) of the failure and generates a technical report instead of treating it as a mishap and completing a mishap report.**

Overview: Changes to NPR 8621.1

New Close Call Definition

Existing Definition

Close Call. An occurrence or a condition of employee concern in which there is no injury or only minor injury requiring first aid and no significant equipment/property damage/mission failure (less than $1000), but which possesses a potential to cause a mishap.

Proposed Definition

Close Call. An event in which there is no injury or only minor injury requiring first aid and/or no equipment/property damage or minor equipment/property damage (less than $1000), but which possesses a potential to cause a mishap in the same location or elsewhere

Overview: Changes in NPR 8621.1

Roles and Responsibilities

Mission Directorate Associate Administrator (MDAA)

- Serve as the appointing official for Type A mishaps, Type B mishaps, high visibility mishaps, and high visibility close calls that involve Mission Directorate programs/projects/activities that occur outside the Center's gates, occur in-flight, or at a Program/Project contractor site that is not managed by a Center

Center Director (CD)

- Serve as the appointing official for Type A mishaps and Type B mishaps occurring at, or managed by, his/her Center and involving off-site Center support contractors.

Chief Engineer

- Concur on Mishap Investigation Board (MIB) membership for Type A mishaps, Type B mishaps, high visibility mishaps, and high visibility close calls (Requirement).

- Serve as an endorsing official for Type A mishaps, Type B mishaps, high visibility mishaps, and high visibility close calls (Requirement).

Overview of Changes to NPR 8621.1

Other Changes

- Close calls involving aircraft may be entered into the Johnson Aircraft Anomaly Reporting System (JAARS) in lieu of IRIS.

- Additions to Program Contingency and Mishap Preparedness Plan:
  - Chain of Custody
  - Expiration Date
  - Submit to Chief OSMA for concurrence 2 weeks prior to SMARR

- For major mishaps such as loss of a Shuttle or significant damage to the Space Station, NASA will not grant privilege to witnesses.

  - When it is expected that an external investigating body will be the sole mishap investigation authority (e.g., for catastrophic vehicle failure such as Space Shuttle or International Space Station loss, or airplane loss), NASA shall not grant privilege to witnesses for either written witness statements or verbal witness statements, even when those statements are taken within the first 24 hours after the mishap (Requirement).

Types of Mishaps

"What can go wrong?"

- **Equipment will fail**
- **Software will contain errors**
- **Humans will make mistakes**
- **Humans will deviate from accepted policy and practices**

There is a lot at stake!

- **Human life**
- **One-of-a-kind hardware**
- **Government equipment & facilities**
- **Scientific knowledge**
- **Public confidence**

Mars Climate Orbiter

Challenger

NOAA N Prime

Columbia

Payload Canister

Helios

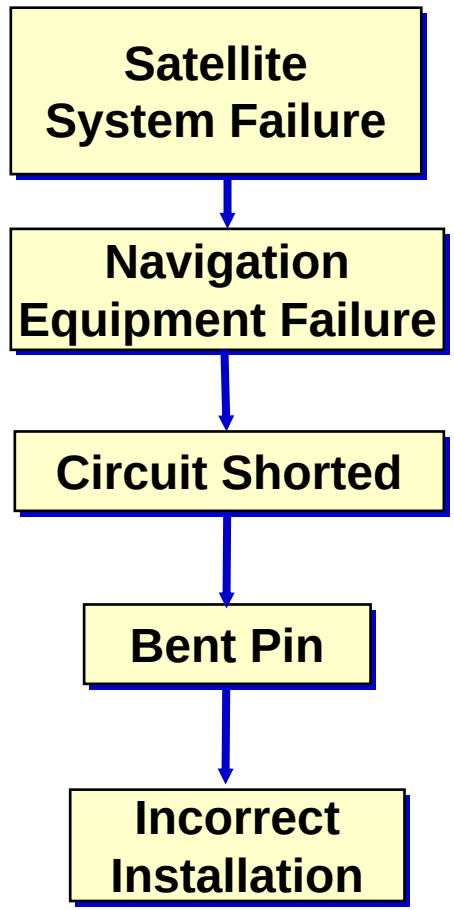
Investigating Causes of Failures & Mishaps

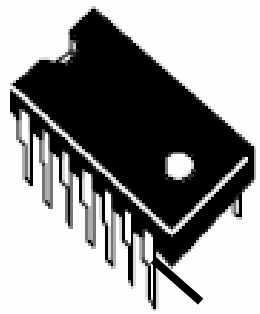
Often investigators:

- **Identify the part or individual that failed.**
- **Identify the type of failure.**
- **Identify the immediate cause of the failure.**
- **Stop the investigation.**

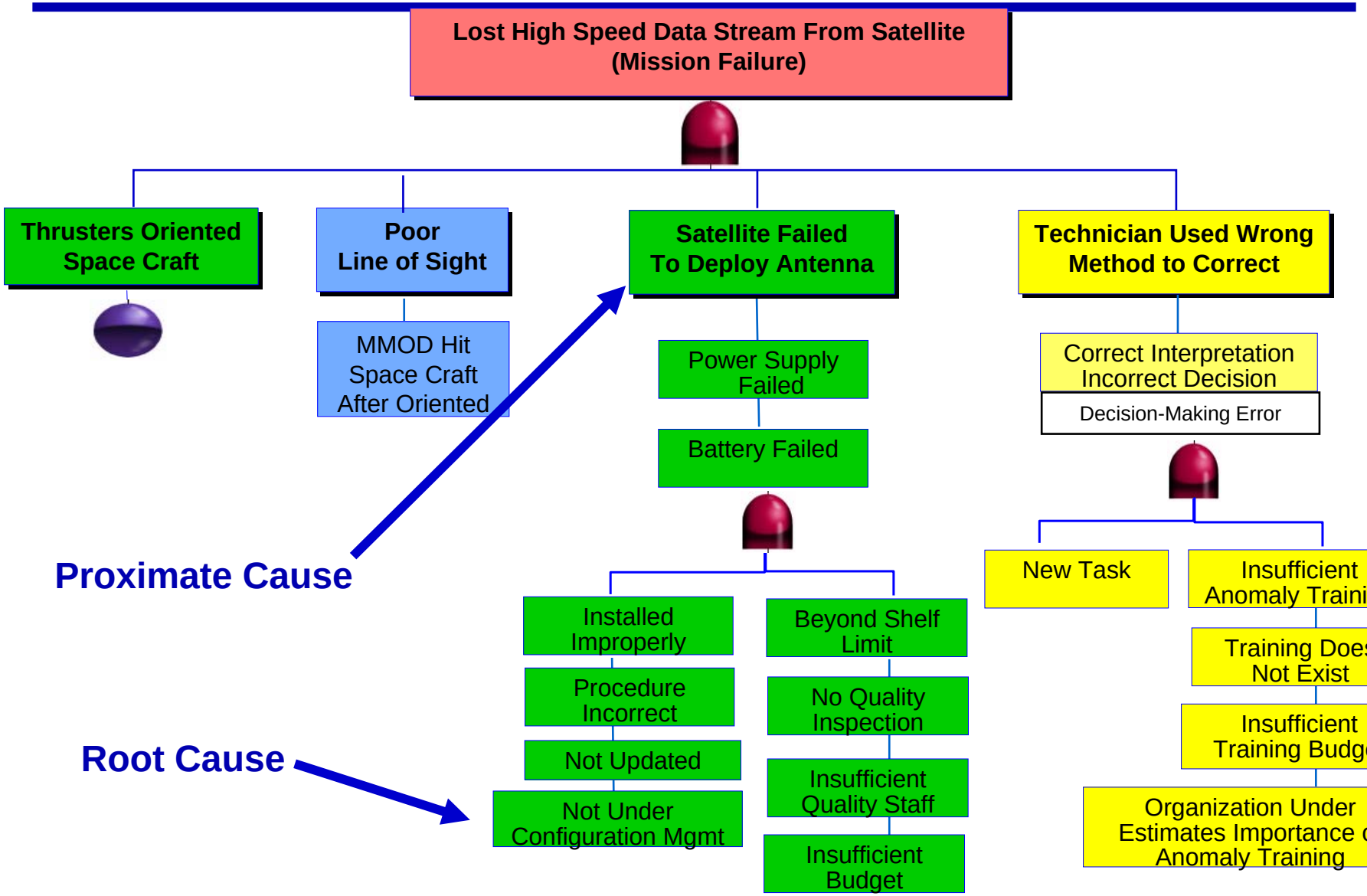
<u>Problem with this approach</u>:

The underlying causes may continue to produce similar problems or mishaps in the same or related areas.



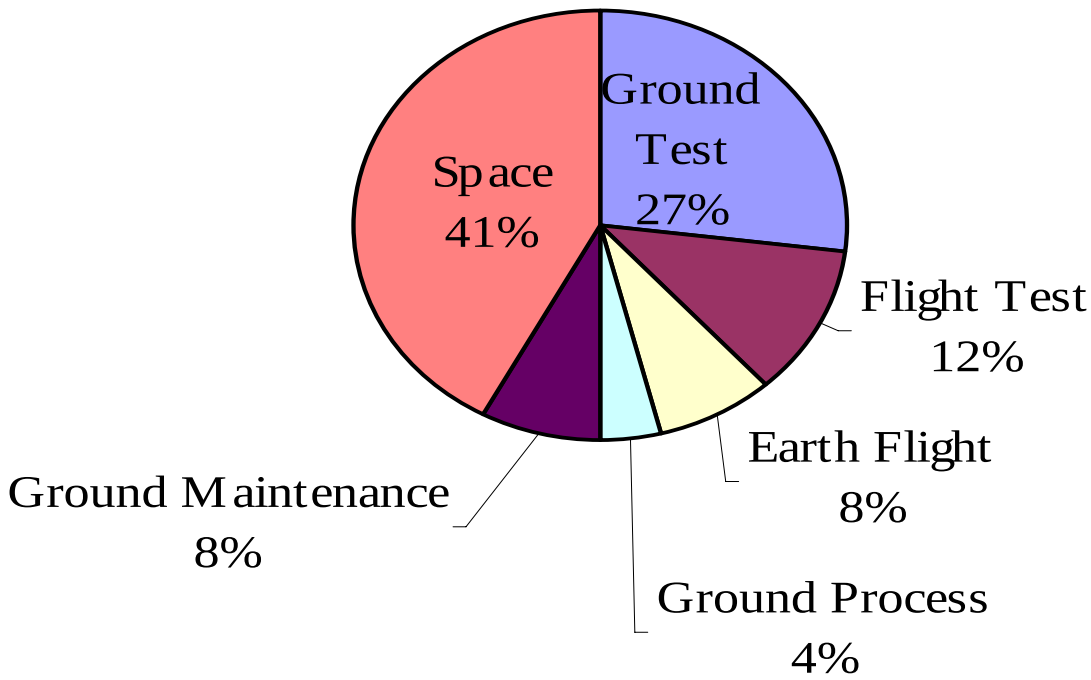


Investigating Causes of Failures & Mishaps

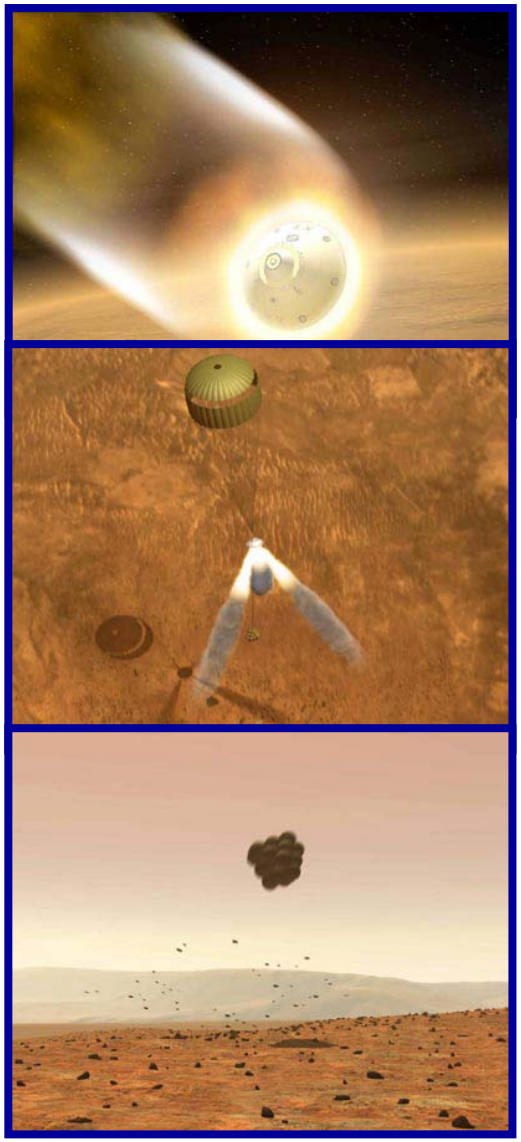


Phase of Life Cycle Where Major Mishaps Have Occurred

Percentage of Type A Mishaps Occurring During Each Type of Activity 1996-2005



Lessons Learned – Close Calls & Mishaps



Mars Exploration Rovers

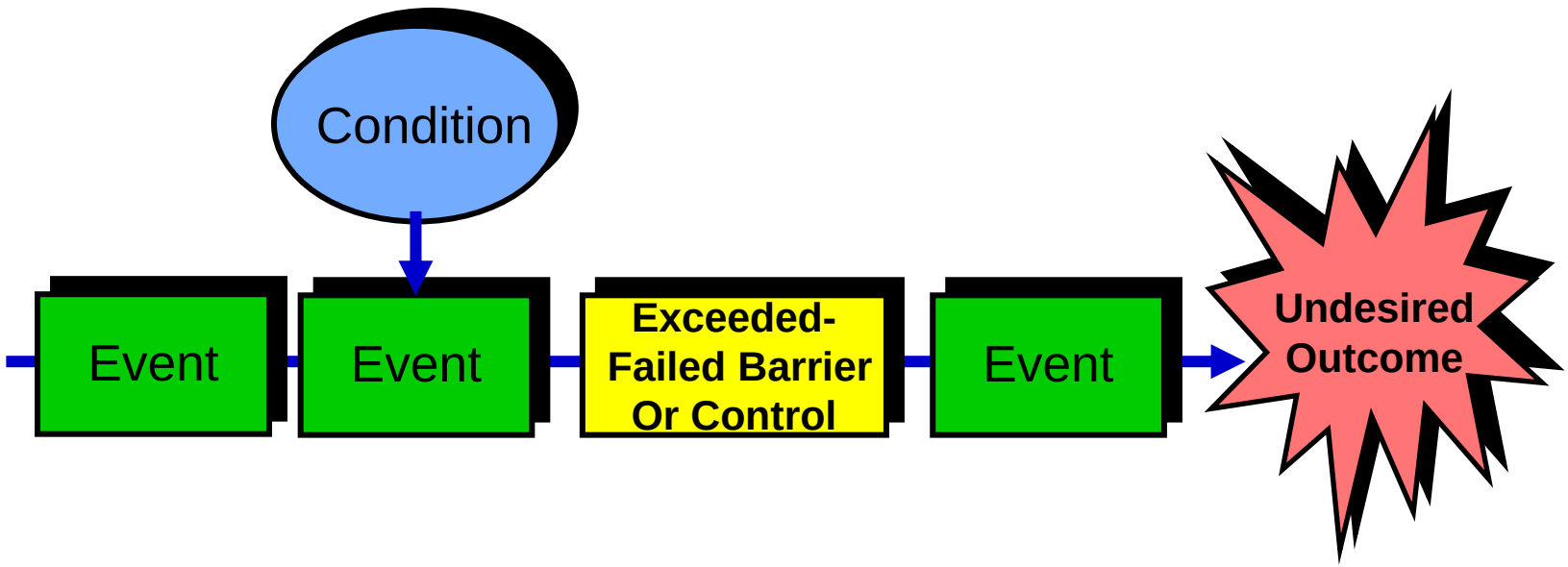
Even Programs with Great Success Have Significant Failures and Close Calls

- **Cancellation of one rover due to concerns about ability to be ready safely for launch.**
- **Air bag failure months before launch.**
- **Parachute failure months before launch.**
- **Potential cable cutter shorting days before launch.**
- **Pyrotechnic firing software concern one day before Mars arrival.**

Lessons Learned – Close Calls & Mishaps

- **Causes of close calls are often similar to mishaps… the difference…**

- **The systems defenses detect and correct the failures and problems or mitigate their consequences….before they lead to mishaps.**



Human Error Causes Mishaps

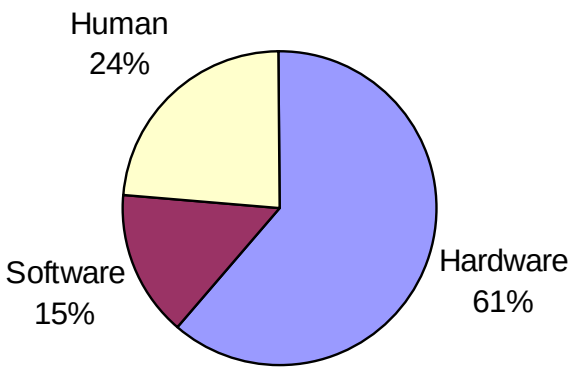
NASA

57% of Type A mishaps caused by human error (1996-2005)

*Does not include auto accidents or death by natural causes

78% of the Shuttle ground-support operations incidents resulted from human error (Perry, 1993).

Proximate Cause of Type A Mishaps in Last 10 Years



Outside NASA

75% of all US military aircraft losses involve sensory or cognitive errors (Air Force Safety Center, 2003).

63% of approach & landing accidents involve inadequate monitoring and cross-checking (Air Force Safety Center, 2003).

83 % of 23,338 accidents involving boilers and pressure vessels were a direct result of human oversight or lack of knowledge (National Board of Boiler and Pressure Vessel Inspectors, 2005).

41% of mishaps at petrochemical plants were caused by human error (R.E. Butikofer, 1986).

Causes of Mishaps – Outside NASA

Causes of Errors in Design Process

(Companies in US & Japan)

- Schedule pressure
- Oversight
- **Lack of testing**
- Changing requirements
- Lack of structure
- **Miscommunication**
- Lack of prototyping

Causes of Errors in Aviation

(FAA Research-119 Accidents)

- Crew resource mis-mgmt.
- Adverse mental states
- Physical/mental limitations
- Inadequate supervision
- Organizational process
- **Failed to correct known problems**

Causes of Errors in Operations

(Aerospace/Aviation Co.)

- **Failure to enforce standards & policies**
- Lack of quality assurance during procedure writing
- Inadequate, confusing procedures
- Duties not understood/ unclear role
- Failure to trend and learn from previous problems
- **Failure to fix known problems**
- Schedule pressure
- Poor communication

Causes of Errors in Maintenance

(FAA Dirty Dozen)

- **Lack of communication**
- Complacency
- Lack of knowledge
- Distraction
- Lack of teamwork
- Fatigue
- Lack of resources
- Pressure
- Lack of assertiveness
- Stress
- Lack of awareness
- Norms

Causes of Mishaps – Inside NASA

Design
• Logic **design error** existed - Design errors in the circuitry were not identified
• **Drawing incorrect**
• **System drawings were incorrect** because they were not updated when system was moved from its original location to the Center.
• System labels were incorrect.
• System did not have sensors to detect failure.
• Configuration changes driven by programmatic and technological constraints… reduced design robustness and margins of safety.

Reviews
• Design was not peer reviewed
• **Systems reviews were not conducted**
• Technical reviews failed to detect error in design
• Red-Team Reviews failed to identify design errors

Tests
• Testing only for correction functional behavior … not for anomalous behavior, especially during initial turn-on and power on reset conditions
• **There was no end-to-end test**.
• Test procedure did not have a step to verify that all critical steps
• Lacked a facility validation test
• **Failed to test as fly….fly as you test**
• **Tests were cut because funding was cut**

Causes of Mishaps – Inside NASA

Operations
• **Team error in analysis** due to lack of system knowledge. This contributed to the team's lack of understanding of essential spacecraft design.
• **Incorrect diagnosis of problem** because the team lacked information about changes in the procedures.
• Emergency step/correction maneuver was not performed.

Communication
• **Inadequate communication** between shifts
• Inadequate communications between project elements

Paperwork
• Lacked documentation on system characteristics
• Processing paperwork and discrepancy disposition paperwork were ambiguous
• **Electronic paperwork system can be edited with no traceability** (Info was changed and no record of the change was recorded).
• Written procedures generally did not have full coverage of the pretest setup and post-test teardown phases of the process
• **Did not follow procedures** (led to death)
• Procedure did not have mandatory steps

Causes of Mishaps – Inside NASA

Supervision
• **"Failure to correct known problems"** was a supervisory failure to correct similar known problems. (Hardware)
• Supervisory Violation" was committed by repeatedly waiving required presence of quality assurance and safety and bypassing Government Mandatory Inspection Points.
• Lacked "organizational processes" to effectively monitor, verify, and audit the performance and effectiveness of the processes and activities.

Staffing
• **Inadequate operation's team staffing**.

Risk Assessment & Risk Mgmt
• **Did not consider the worst-case effect**. Lacked systematic analyses of "what could go wrong."
• The perception that operations were routine resulted in inadequate attention to risk mitigation.
• The project was not fully aware of the **risks** associated with the test.
• Lack of adequate analysis methods led to an inaccurate risk assessment of the effects of configuration changes.

Conclusion from Study

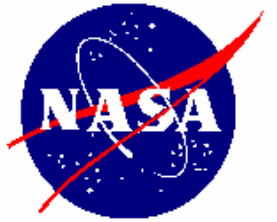
- Lots of times we're lucky or prepared and we dodge the bullet...
- But sometimes we endure very public failures, loss of life and significant loss of property...
- In the majority of these cases, we experience the mishap because hardware, software or human failures occurred, and our controls (systems defenses) did not detect and correct these before the mishap.
- When failures occur, we try to learn from them.
- To be successful, we must report and investigate our failures… identify the underlying root causes and generate solutions that prevent these systemic problems from creating more failures… in our program… and in others.

For More Information

- NASA PBMA Mishap Investigation Website
  (http://ai-pbma-kms.intranets.com/login.asp?link=)
  - Includes:
    - Links (e.g, to Root Cause Analysis Software, a RCA Library).
    - Documents (e.g., Methods, Techniques, Tools, Publications and Presentations).
    - Threaded Discussions and Polls.

- SOLAR Course: "Introduction to Mishap Investigation"

- HQ Office of Safety & Mission Assurance
  - Faith.T.Chandler@nasa.gov



Backup

Mishap Classification Levels

Classification Level	Property Damage	Injury
Type A	Total direct cost of mission failure and property damage is **$1,000,000 or more**, ***or*** Crewed aircraft hull loss has occurred, ***or*** Occurrence of an unexpected aircraft departure from controlled flight (except high performance jet/test aircraft such as F-15, F-16, F/A-18, T-38, and T-34, when engaged in flight test activities).	Occupational injury and/or illness that resulted in: A fatality, ***or*** A permanent total disability, ***or*** The hospitalization for inpatient care of 3 or more people within 30 workdays of the mishap.
Type B	Total direct cost of mission failure and property damage of at least $250,000 but less than $1,000,000.	Occupational injury and/or illness has resulted in permanent partial disability. ***or*** The hospitalization for inpatient care of 1-2 people within 30 workdays of the mishap.
Type C	Total direct cost of mission failure and property damage of at least $25,000 but less than $250,000.	Nonfatal occupational injury or illness that caused any workdays away from work, restricted duty, or transfer to another job beyond the workday or shift on which it occurred.
Type D	Total direct cost of mission failure and property damage of at least $1,000 but less than $25,000.	Any nonfatal OSHA recordable occupational injury and/or illness that does not meet the definition of a Type C mishap.
Close Call	Total direct cost of mission failure and property damage is less than $1,000 ***or*** An occurrence or condition of employee concern in which there is no property damage but possesses the potential to cause a mishap.	Minor injury requiring first aid which possesses the potential to cause a mishap ***or*** An occurrence or condition with no injury but possesses the potential to cause a mishap.

Preparing for Mishaps: Pre-Mishap Plans

- **Center Pre-Mishap Plan**
  - Local close call and mishap reporting & investigating procedures
  - Center specific emergency response
  - Procedures to appoint an Interim Response Team
  - Location of space for impounded objects
  - Mishap process to establish investigating authority and process report (Type C mishaps, Type D mishaps, and close calls)

- **Program Pre-Mishap Plan**
  - Specific procedures for program emergency response and investigating (e.g., safing procedures, toxic commodities, …)
  - Names chair and ex-officio for a Type A board.
  - Procedures to impound data, records, etc… for off-site mishaps
  - Identifies national, state, and local organizations and agencies which are most likely to take part in debris collection
  - Identifies MOUs with international partners and agencies that may support investigation